1/ RP9

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/454,646 | 12/06/1999 | David Carroll Challener | RP9-98-055 | 4026 |

25299 7590 07/10/2003

IBM.CORPORATION
PO BOX 12195
DEPT 9CCA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

| EXAMINER | |
|---|---|
| KIM, JUNG W | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2132 | 8 |

DATE MAILED: 07/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/454,646 | CHALLENER ET AL. | |
| | Examiner | Art Unit | |
| | Jung W Kim | 2132 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) 1-11 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-11 is/are rejected.

7)☒ Claim(s) 3 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 06 December 1999 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

## DETAILED ACTION

### *Drawings*

1. The drawings are objected to because on figure 1, the reference sign pointing to the personal computer monitor is labeled "17" but referred to in the specification as "11". A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

2. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. Figure 1 is objected to under 37 CFR 1.83(a) because it fails to show covers which may be secured against tampering as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in

the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

5. Applicant is required to submit a proposed drawing correction in reply to this Office action. However, formal correction of the noted defect may be deferred until after the examiner has considered the proposed drawing correction. Failure to timely submit the proposed drawing correction will result in the abandonment of the application.

***Specification***

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

2. The disclosure is objected to because of the following informalities: on page 24, line 7 under the Abstract, the phrase "will turn of the system" should read "will turn off the system"; on page 2, lines 7-8 under the subsection "Background Art", the sentence is not grammatical; on page 5, line 17 under the section "Summary of the Invention", the phrase "personal; computer" should read "personal computer"; on page 7, line 16, the phrase "who us responsible" should read "who is responsible"; on page 8, lines 4-5 under the section "Detailed Description of the Preferred Embodiment", the sentence "The System Owner will also have to record all attempted security breaches." implies that the administrator is omniscient in regards to perceiving attempted security breaches-the sentence should be rewritten to suggest that the System Owner will record all known attempted security breaches; on page 13, line 15 under the section "Detailed Description of the Preferred Embodiment", the sentence is not grammatical;

on page 14, lines 9-13, the sentence is not grammatical; on page 16, line 8 under the section "Detailed Description of the Preferred Embodiment", there is a redundant comma in the sentence. Appropriate correction is required.

### *Claim Objections*

1. Claim 3 is objected to because of the following informalities: the phrase "use of a password different that the password of a normal user" should read "use of a password different then the password of a normal user". Appropriate correction is required.

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. Claims 1-9 are rejected under 35 U.S.C. 102(a) as being anticipated by Frisch (Essential System Administration). Methodologies for establishing levels of security as disclosed by the applicants in claim 1 are found in several OS systems. The security system integrated in the Unix OS is an example. Referring to claims 1-6, Frisch discloses how Unix stores user profile information utilizing various methodologies. Users are given their own unique id as well as at least one group id, which defines for each user a security access level (see Frisch, page 146). Moreover, user and group ids are located in the passwd and group files in the /etc/ directory of a Unix system (see

Frisch, page 146). Associated with each user id are distinct usernames and passwords. This information is used in multiple security-driven events including user login and administration of file read, write, and execute permissions (see Frisch, pages 25-36). Of the users, the root user is afforded the highest security level and can read, write, and execute any file on the system; thereby enabling the root user to change both the passwd and group files, and hence alter the security of the system to a lower state (see Frisch, page 5). Moreover, by creating a file system where all directories and files except those found in the /usr/local/home/ (this directory typically stores user account directories) are owned by the root user, permissions to read, write, and execute all files other than those located in the user account directories are controlled by this super user; only the root user can change the security of the system to a lower state. In addition, Unix allows a "normal user" (one without root access) to establish a more secure state. Examples of normal user defined activity include writing cron jobs to periodically log the account activity or changing file permissions on files owned by the user to more secure levels (see Hirsch, pages 381-386 and pages 25-36). Furthermore, Hirsch discloses a feature to log unsuccessful login attempts. Under the AIX version of Unix, the /etc/security/user file lists several login profile attributes for each user including: the time of the last login, unsuccessful login count, time of the last unsuccessful login, and the host machine of the last unsuccessful login (see Frisch, page 262). Upon inspection of the /etc/security/user file, an administrator can deny a user having a suspicious login profile from accessing the operating system. Finally, although Frisch does not teach using binary indicators to set the secure state level,

binary fields are the standard in the industry for storing any digital information. As mentioned above, normal users can change file permissions they own to more secure states and the root user can alter the state of a system to less secure states by making file access less restrictive. Both of these changes would be reflected in memory as binary manipulations.

3. Referring to claims 7-9, as mentioned above, the Unix operating system implements a security profiling system which covers the following: files /etc/passwd and /etc/group store individual user id and users group association; the user id and group associations allocates permissions to read, write, and execute files; /etc/security/user files stores user login profiles; each user can modify the read, write, and execute permissions on files they own, with the root user able to modify all files (see Frisch, pages 5, 25-36, 146, 262). Moreover, by setting ownership of all files, except those in the /usr/local/home directory, to root, only the root user can alter user shared resources from a more restrictive level to a lesser one. This construction also enables each user to make files in their own home directory more restrictive by altering the permissions for each of the files they own. Finally, the administrator can implement any one or combination of the following in response of a security risk: alter the permissions for a subset of the files to a more secure level, update the /etc/passwd and /etc/group files by deleting suspicious accounts, and broaden the login monitoring system utilizing various logging features.

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Frisch as applied to claims 7-9 above, and further in view of Schmidt U.S. Patent No. 5,912,621. Frisch covers a security methodology implemented in a personal computer as defined above in the claim 7-9 rejections under 35 U.S.C. 102(a). However, Frisch does not define a response by the operating system when the cover of the computer is removed. A response by a computer system when a cover is removed is given by Schmidt. Schmidt teaches a need to protect a computer from physical threats in addition to the protection offered by conventional login and network intrusion detection systems (see Schmidt, col. 1, lines 1-10 and lines 35-50). Schmidt's invention to meet these needs is a computer cabinet security state detection system whereby an auxiliary state element changes state in response to the cover being opened. A state program is run when the auxiliary state element detects the cover being removed to poll the status of the element. This state report is further submitted to security personal for examination (see Schmidt, col. 1, line 51-col. 2, line 7). Administrators would then be able to adjust the security profile if the report shows suspicious activity. It would be obvious to one with ordinary skill in the art at the time the invention was made to include the computer cabinet security state detection system with the Linux operating system

since physical threats should be addressed to prevent tampering of the physical devices of a computer, and thereby enabling a more robust computer security system.

3. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Frisch in view of Lapointe U.S. Patent No. 5,606,615. As mentioned in the earlier claim rejections under 35 U.S.C. 102(a), Frisch teaches a security system implemented in the Unix operating system. One embodiment of the system locks the user account after a specified number of consecutive incorrect password attempts (see Frisch, page 160, table). Moreover, only the root user can define computer operational modes at computer startup (see Frisch, pages 86-90). Finally, the /etc/passwd and /etc/group determine login access as well as file ownership and read/write/access privileges (see Frisch, pages 25-36). However, Frisch is silent on the matter of powering down the computer after a user supersedes the predefined number of consecutive unsuccessful login attempts. Lapointe does disclose such a computer system that powers down when an unauthorized user attempts to access a computer with an electronic key (see Lapointe, col. 6, lines 9-12). Although Lapointe's method to restrict access to a computer using an electronic key differs from Frisch's password system, both are methodologies to provide access for predetermined users. Therefore, it would obvious to one with ordinary skill in the art at the time the invention was made to power down the computer when a user surpasses the threshold number of consecutive unsuccessful login attempts since power down further secures the operating system from login attempts by any user except the root user. This power shutoff system would enable the

computer to prevent malicious intruders from repeated, consecutive login attempts using several usernames and thus make the computer more secure.

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cromer U.S. Patent Number 6,357,007 discloses a system for detecting tamper events.

Kuo U.S. Patent Number 6,289,456 discloses a hood intrusion methodology.

Morgan, Andrew G. 'Pluggable Authentication Modules for Linux', Linux Journal, Specialize Systems Consultants, Inc. January 1997. Retrieved from: ACM Portal.

Frisch, AEleen 'Linux Systems Administration: Maximizing System Security, Part 1', Linux Journal, Specialize Systems Consultants, Inc. January 1996. Retrieved from: ACM Portal.

Frisch, AEleen 'Linux Systems Administration: Maximizing System Security, Part 2', Linux Journal, Specialize Systems Consultants, Inc. January 1996. Retrieved from: ACM Portal.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is 703-305-8289. The examiner can normally be reached on M-F 8:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-9939 for regular communications and 703-746-9939 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Jung W Kim
Examiner
Art Unit 2132

jk
July 8, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100